

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 712 768 A1

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
22.05.1996 Patentblatt 1996/21

(51) Int. Cl.⁶: **B60R 25/04**

(21) Anmeldenummer: **95114014.4**

(22) Anmeldetag: **07.09.1995**

(84) Benannte Vertragsstaaten:
ES FR GB IT

(71) Anmelder: **MERCEDES-BENZ AG**
D-70327 Stuttgart (DE)

(30) Priorität: **17.11.1994 DE 4440975**

(72) Erfinder: **Büdel, Ulrich, Dipl.-Ing.**
D-70771 Leinfelden-Echterdingen (DE)

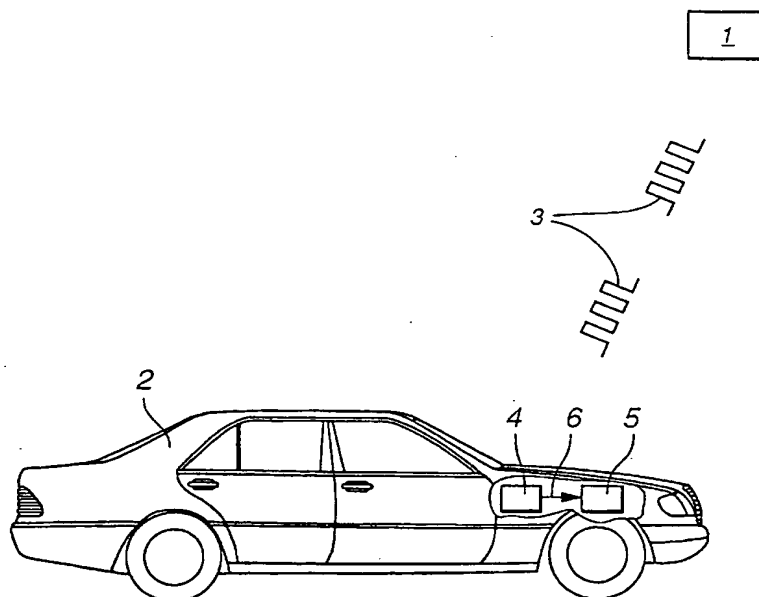
(54) **Fremdnutzungsschutzeinrichtung für ein Kraftfahrzeug**

(57) 2.1. Es sind Einrichtungen dieser Art als Wegfahrsperrern bekannt, bei denen eine fahrzeugeitig angeordnete Nutzungssteuerungseinrichtung ein oder mehrere fahrbetriebsnotwendige Fahrzeugaggregate in Abhängigkeit von einer auf einer Benutzerkarte abgespeicherten, über einen Kartenleser zuführbaren, fahrzeugspezifischen Nutzungsberechtigungsinformation betriebsbereit oder deaktiviert hält. Zudem sind Wegfahrsperrern bekannt, die über ein Funksignal ferngesteuert ausgelöst werden können.

2.2. Es wird eine Fremdnutzungsschutzeinrichtung vorgeschlagen, bei der die Nutzungsberechtigungsinformation von einer Sendeanlage auf der Basis elektroma-

gnetischer Wellen im vorgegebenen Fahrzeugnutzungsgebiet abgestrahlt wird und periodisch aufeinanderfolgende Nutzungssignale enthält und bei der die Nutzungssteuerungseinrichtung das oder die fahrbetriebsnotwendigen Fahrzeugaggregate nach Empfang eines Nutzungssignals jeweils nur für eine vorgegebene anschließende Zeitdauer betriebsbereit hält, während sie den weiteren Fahrbetrieb bei Ausbleiben der Nutzungssignale sperrt.

2.3. Verwendung z.B. zum Schutz vor unberechtigter Fremdnutzung von Personenwagen.



BEST AVAILABLE COPY

EP 0 712 768 A1

Beschreibung

Die Erfindung bezieht sich auf eine Fremdnutzungsschutzeinrichtung für ein Kraftfahrzeug, die eine fahrzeugseitig angeordnete Nutzungssteuerungseinrichtung beinhaltet, welche den Betriebszustand wenigstens eines fahrbetriebsnotwendigen Fahrzeugaggregates in Abhängigkeit von einer zugeführten, fahrzeugspezifischen Nutzungsberechtigungsinformation steuert.

Eine solche Einrichtung ist z.B. in der Patentschrift US 4 805 722 offenbart. Die dortige Nutzungssteuerungseinrichtung steuert unter anderem die Zündung sowie die Benzinzufuhr für ein Kraftfahrzeug mit Verbrennungsmotor. Diese Steuerung erfolgt in Abhängigkeit von einer eingangsseitig über einen Kartenleser zuführbaren Nutzungsberechtigungsinformation, die wenigstens eine Fahrzeugidentitätsinformation sowie eine Nutzungsdauerinformation umfaßt, die mittels des Kartenlesers von einer einführbaren Benutzerkarte ablesbar sind. Die Nutzungssteuerungseinrichtung vergleicht diese Informationen bei einem Fahrzeugstart mit einer in ihr gespeicherten Fahrzeugidentitätsinformation und der von einem eigenen Zeitgeber generierten Zeitinformation über das momentane Datum und die momentane Uhrzeit. Erkennt sie bei diesem Vergleich, daß die Fahrzeugidentitäten nicht übereinstimmen oder daß die auf der Karte gespeicherte Nutzungsdauer abgelaufen ist, sperrt sie den weiteren Fahrzeugbetrieb durch Unterbrechen der Benzinzufuhr und Deaktivierung der Zündung. Ein solches System auf der Basis einer Benutzerkarte birgt ebenso wie zugangsblockierende Systeme in Form von Schließanlagen mit mechanischem und/oder elektrischem Schlüssel die Gefahr, daß sich ein unberechtigter Fremdnutzer durch Bedrohung des Berechtigten in den Besitz des nutzungsberechtigenden Elementes, d.h. der Karte oder des Schlüssels, sowie der ggf. zur weiteren Nutzung erforderlichen Benutzercodeinformation bringt.

Um einer solchen Gefahr der Fahrerbedrohung zu begegnen, ist bereits vorgeschlagen worden, eine fahrzeugseitig angeordnete Wegfahrsperrung erst nach einem Diebstahl über ein Funksignal, das z.B. durch die Herstellerfirma ausgelöst werden könnte, zu aktivieren, so daß sich wegen des zunächst erfolgreichen Diebstahlversuchs für den Unberechtigten kein Anlaß zur Bedrohung des Berechtigten ergibt. Allerdings bleibt dieser Fremdnutzungsschutz unwirksam, wenn es dem Unberechtigten erfolgreich gelingt, zwischenzeitlich Maßnahmen zur Abschirmung des zum Empfang des Funksignals der Wegfahrsperrung vorgesehenen Empfängers im Fahrzeug vorzunehmen.

Weiter ist es bekannt, einen indirekten Fremdnutzungsschutz dadurch zu erreichen, daß das Fahrzeug mit einem Satelliten-Ortungssystem, z.B. einem sog. GPS-System, ausgerüstet wird, um auf diese Weise jederzeit geortet werden zu können, siehe z.B. den Beitrag "Satellitenhilfe gegen Auto-Klau" von R. Gramm in der Zeitschrift Funkschau 16/1993, Seite 42. Die Ver-

wendung eines solchen Ortungssystems erfordert jedoch einen nicht unbeträchtlichen Aufwand und ist zudem vom Standpunkt des Datenschutzes her nicht unproblematisch.

Aus der Patentschrift DE 42 40 458 C1 ist eine weitere Einrichtung der eingangs genannten Art bekannt, bei der ein im Zündschlüssel des Kraftfahrzeuges integrierter Code-Sender periodisch Signale aussendet, wenn die Zündung eingeschaltet ist. Ein in einem elektronischen Gerät im Kraftfahrzeug integrierter Code-Empfänger empfängt diese Code-Signale bei eingeschalteter Zündung und wertet sie aus. Bei fehlendem oder fehlerhaftem Code-Signal gibt er Alarm. Dabei kann vorgesehen sein, daß der Code-Empfänger mit der Kraftfahrzeugelektronik verbunden ist und im Alarmfall funktionswesentliche Elemente des Kraftfahrzeuges gesperrt werden. Zudem wird dort vorgeschlagen, bei Bedarf mehrere, sich in einem Fahrzeug befindende elektronische Geräte mit je einem Code-Empfänger auszustatten und so auszulegen, daß funktionswesentliche Baugruppen des elektronischen Gerätes abgeschaltet werden, wenn kein Code-Signal im Code-Empfänger empfangen werden kann.

In der Offenlegungsschrift DE 42 39 271 A1 ist eine Diebstahlsicherung mit Sende-Empfangs-Prinzip offenbart, bei der ein zu überwachender Gegenstand, insbesondere ein Fahrzeug, einen Empfänger mit einer individuellen Adresse erhält und bei Empfang seiner Adresse, die über einen außerhalb des Gegenstandes angeordneten Sender gesendet wird, ein im Gegenstand befindlicher Sender aktiviert wird, der daraufhin Signale aussendet, die mit mindestens einem weiteren außerhalb des Gegenstandes angeordneten Empfänger empfangen und ausgewertet werden. Der Sender außerhalb des zu überwachenden Gegenstandes kann beispielsweise ein Rundfunksender sein. Die außerhalb des Gegenstandes vorgesehenen Empfänger befinden sich im Fall der Überwachung eines Kraftfahrzeuges über die Landschaft verteilt an Autobahnauffahrten, Tankstellen, Ortseingängen usw.. Das von dem im Gegenstand befindlichen Sender ausgesandte Signal wird von den außerhalb des Gegenstandes befindlichen Empfängern daraufhin ausgewertet, wo sich dieser Sender und damit der zu überwachende Gegenstand befindet, um den zu überwachenden Gegenstand jederzeit lokalisieren zu können.

Der Erfindung liegt als technisches Problem die Bereitstellung einer Fremdnutzungsschutzeinrichtung zugrunde, welche einen hohen Diebstahlschutz bietet, komfortabel und funktionssicher ist, den berechtigten Fahrzeugbenutzer nicht gefährdet und außerdem nicht durch Abschirmungsmaßnahmen gegenüber zum Fahrzeug gesendeten Signalen außer Funktion gesetzt werden kann.

Dieses Problem wird durch eine Fremdnutzungsschutzeinrichtung mit den Merkmalen des Patentanspruchs 1 gelöst. Bei dieser Einrichtung ist vorgesehen, Nutzungssignale periodisch aufeinanderfolgend von einer fahrzeugexternen Stelle über eine Übertragungs-

strecke auf der Basis elektromagnetischer Wellen auszusenden und eines

oder mehrere fahrbetriebsnotwendige Fahrzeugaggregate durch die Nutzungssteuerungseinrichtung jeweils auf ein von letzterer empfangenes Nutzungssignal hin nur für eine vorgegebene Zeitdauer größer als der Zeitabstand zweier aufeinanderfolgender Nutzungssignale betriebsbereit zu halten, während ihr weiterer Betrieb und damit derjenige des Kraftfahrzeuges insgesamt gesperrt wird, sobald während dieser vorgegebenen Zeitdauer kein weiteres Nutzungssignal empfangen wird. Anstelle der Übertragung von nutzungsverhindernden Funksignalen, wie im Fall der bekannten, funksignalaktivierten Wegfahrsperre, werden hier umgekehrt nutzungsberechtigte Signale empfangen. Damit ist die Einrichtung automatisch vor Abschirmmaßnahmen gegenüber den zum Fahrzeug gesendeten Signalen durch einen Unberechtigten gesichert, da es hier im Interesse des jeweiligen Fahrzeugnutzers liegt, daß das Signal möglichst störungsfrei empfangen wird.

Bei einem Diebstahl meldet der Berechtigte denselben bei der für die Ausstrahlung der Nutzungssignale autorisierten Stelle, die daraufhin das weitere Aussenden von Nutzungssignalen einstellt, wonach die Nutzungssteuerungseinrichtung den weiteren Fahrzeugbetrieb blockiert. Dies kann entweder unmittelbar nach dem Ausbleiben eines Nutzungssignales oder nach Ablauf eines weiteren Zeitintervalls geschehen, wobei letzteres ggf. aus Funktionssicherheits- und/oder Verfügbarkeitserwägungen vorteilhaft sein kann. Eine solche autorisierte Stelle kann z.B. durch eine staatliche Stelle wie die Polizei oder durch den Fahrzeughersteller gebildet sein. Da die Nutzungsberechtigungsinformation fahrzeugextern über eine oder mehrere Sendeeinheiten mittels elektromagnetischer Wellen abgestrahlt wird, läßt sich ohne Zusatzaufwand durch geeignete Wahl des erreichbaren Sendegebietes das Nutzungsgebiet für das jeweilige Fahrzeug in gewünschter Weise vorgeben, insbesondere auf einen bestimmten Raum, wie z.B. Deutschland oder Europa, beschränken. Da der Berechtigte keinen direkten Einfluß auf die Abstrahlung der Nutzungssignale hat, entfällt die Gefahr einer Bedrohung desselben durch einen Unberechtigten. Diese Bedrohungsgefahr für den Fahrzeugbesitzer ist zudem dadurch minimiert, daß das Fahrzeug außer vom Besitzer ggf. auch von einer anderen Person als entwendet gemeldet und anschließend von der autorisierten Stelle stillgesetzt werden kann. Die Einrichtung kann zudem Schutz vor einem betrügerisch initiierten Diebstahl durch den Berechtigten selbst bieten, indem die Versicherung, wenn der Berechtigte sein Fahrzeug bei ihr als gestohlen meldet, bei der autorisierten Stelle das Aussetzen der Abstrahlung weiterer Nutzungssignale für dieses Fahrzeug anfordert. Das als gestohlen gemeldete Fahrzeug kann folglich nicht mehr benutzt und damit vom gegenwärtigen Besitzer auch nicht mehr zur weiteren aktiven Benutzung veräußert werden.

In Ausgestaltung der Erfindung werden gemäß Anspruch 2 die Nutzungssignale über ein digitales Funk-

netz übertragen. Hierzu können bereits bestehende Funknetze verwendet werden, so daß die Einrichtung einer separaten Übertragungsstrecke nicht erforderlich ist. In weiterer Ausgestaltung dieser Maßnahme bildet gemäß Anspruch 3 ein Autotelefon den Empfangsteil der Nutzungssteuerungseinrichtung, wobei das Autotelefon parallel seine übliche Funktion zusätzlich erfüllt. Damit entfällt die Notwendigkeit eines separaten Empfangsteils für die Fremdnutzungsschutzeinrichtung für Fahrzeuge, die bereits mit Autotelefon ausgerüstet sind.

Eine bevorzugte Ausführungsform der Erfindung ist in der Zeichnung dargestellt und wird nachfolgend beschrieben.

Die einzige Figur zeigt schematisch eine Fremdnutzungsschutzeinrichtung mit Nutzungssignalübertragung in einem Blockdiagramm.

In der Figur ist schematisch eine Sendeanlage (1) dargestellt, die für hierzu registrierte Fahrzeuge, von denen eines (2) schematisch gezeigt ist, fahrzeugspezifische Nutzungsberechtigungsinformationen über ein digitales Funknetz (3) in einem vorgegebenen Fahrzeugnutzungsgebiet abstrahlt, wobei die Sendeanlage (1) mehrere räumlich getrennte Sender umfaßt. Die abgestrahlte Nutzungsberechtigungsinformation enthält Nutzungssignale in Form einer jeweiligen Signalimpulsgruppe von fahrzeugspezifischer Gestalt, wobei die Nutzungssignale in vorgegebenen Zeitabständen periodisch aufeinanderfolgend abgestrahlt werden. Die Sendeanlage (1) kann außer als terrestrische Sendeanlage auch als Satellitensendeanlage realisiert sein.

Fahrzeugseitig beinhaltet die Fremdnutzungsschutzeinrichtung eine Nutzungssteuerungseinrichtung (4) und eine Vielzahl von fahrbetriebsnotwendigen Fahrzeugaggregaten, von denen eines (5) stellvertretend dargestellt ist. Diese Fahrzeugaggregate (5) können beispielsweise durch die verschiedenen, in der Elektrik des Fahrzeugs (2) vorhandenen Steuergeräte realisiert sein, wie z.B. ein vorhandenes Motorsteuergerät. Jedes dieser in die Fremdnutzungsschutzeinrichtung einbezogenen, fahrbetriebsnotwendigen Fahrzeugaggregate (5) ist durch die Nutzungssteuerungseinrichtung (4) über eine zugehörige, manipulationsgeschützte Steuerleitung (6) in ihrem Betriebszustand zwischen freigegebenem Betrieb und gesperrtem Betrieb umschaltbar. Bei Fahrzeugen, die über einen Steuergerätedatenbus verfügen, kann die Signalleitung (6) bevorzugt als Teil dieses Bussystems realisiert sein. Gegebenenfalls kann unter Wegfall einer extern verbindenden Steuerleitung (6) die Nutzungssteuerungseinrichtung (4) in jedes der einbezogenen Fahrzeugaggregate (5) als ein jeweiliger Teil hiervon integriert sein, um die Manipulationssicherheit weiter zu erhöhen. Solche Details der fahrzeugseitigen Realisierung einer solchen zentralen oder dezentralen Wegfahrsperrefunktion von Fahrzeugaggregaten sind Stand der Technik und bedürfen daher vorliegend keiner eingehenden Beschreibung. Insbesondere ist bei der Realisierung dieses fahrzeugseitigen Funktionsteils der Wegfahrsperre darauf zu achten, daß er

nicht durch einfaches Auswechseln einzelner Teile oder Fahrzeugkomponenten umgangen werden kann.

Die Nutzungssteuerungseinrichtung (4) umfaßt des weiteren ein Empfängerteil, das durch ein im Fahrzeug (2) vorhandenes Autotelefon als in die Nutzungssteuerungseinrichtung (4) einbezogene Einheit gebildet wird. Selbstverständlich kann für Fahrzeuge ohne Autotelefon ein separates Empfängerteil für die Fremdnutzungsschutzeinrichtung vorgesehen werden. Immer bei Empfang eines neuerlichen Nutzungssignals und Erkennung desselben als zum betreffenden Fahrzeug (2) gehörig, wozu die Nutzungssteuerungseinrichtung (4) die Fahrzeugidentitätsinformation des empfangenen Nutzungssignals mit einer in ihr gespeicherten Fahrzeugidentitätsinformation vergleicht, hält die Nutzungssteuerungseinrichtung (4) die fahrbetriebsnotwendigen Fahrzeugaggregate (5) jeweils für eine vorgegebene anschließende Zeitdauer in aktivem Betrieb, wobei diese vorgegebene Zeitdauer größer als der Zeitabstand zweier aufeinanderfolgend gesendeter Nutzungssignale ist. Je nach gewünschter Übertragungssicherheit kann diese freigegebene Aggregatbetriebsdauer ein Vielfaches dieses Nutzungssignalzeitabstandes betragen. Wird innerhalb dieser freigegebenen Aggregatbetriebsdauer kein weiteres Nutzungssignal mehr empfangen, so werden die betroffenen Fahrzeugaggregate (5) von der Nutzungssteuerungseinrichtung (4) noch über ein vorgegebenes Zeitintervall hinweg betriebsbereit gehalten, damit sich keine sicherheitskritischen Fahrzustände oder Verfügbarkeitsprobleme ergeben. Nach Ablauf dieses Zeitintervalls werden dann die betroffenen Fahrzeugaggregate (5) von der Nutzungssteuerungseinrichtung (4) nach dem nächsten Stehen des Fahrzeugs (2), z.B. dem nächsten Abschalten der Zündung, in ihren betriebsblockierten Zustand gesteuert, so daß das Fahrzeug nicht mehr in Fahrbereitschaft gesetzt werden kann.

Ein solches Ausbleiben der den Fahrzeugbetrieb aufrechterhaltenden Nutzungssignale kann bei der für die Abstrahlung der Nutzungsberechtigungsinformation autorisierten Stelle, z.B. der Polizei, veranlaßt werden, z.B. vom Berechtigten oder dessen Versicherung, nachdem das Fahrzeug als gestohlen gemeldet wurde. Weiterhin kann das Ausbleiben von Nutzungssignalen darauf zurückzuführen sein, daß sich das Fahrzeug aus dem durch die Reichweite der Sendeanlage (1) festgelegten Nutzungsgebiet entfernt hat. Durch Festlegen gewünschter Nutzungsgebiete läßt sich folglich das Entwerden und Verschieben von Fahrzeugen in andere Länder und/oder Kontinente wirksam unterbinden. Am Instrumentenbrett ist eine entsprechende Warnanzeige, z.B. als Kontrollampe oder alphanumerische Anzeige, vorgesehen, um den Fahrzeugbesitzer vom Ausbleiben der Nutzungssignale zu informieren und ihm innerhalb des eingeräumten Zeitintervalls die Möglichkeit zu geben, eine Werkstatt aufzusuchen. Dort kann festgestellt werden, ob es sich um eine Funktionsstörung der Fremdnutzungsschutzeinrichtung handelt. Bei Bedarf kann zudem die Möglichkeit einer Notinbetriebnahme,

z.B. einmalig nach Auslösen der Wegfahrsperrfunktion oder für eine vorgegebene Zeitdauer danach, vorgesehen werden.

Die Übertragung der Nutzungssignale über das Funknetz (3) ist bereits dadurch weitestgehend manipulationssicher, daß es weder dem Berechtigten noch vor allem einem Unberechtigten möglich sein dürfte, aus der Vielzahl abgestrahlter Nutzungssignale für die verschiedenen Fahrzeuge das für das betreffende Fahrzeug vorgesehene zu erkennen, um es anderweitig zu generieren und damit das System umgehen zu können. Falls gewünscht, kann zusätzlich eine codesgeschützte Nutzungssignalübertragung eingerichtet werden, wie sie z.B. für die Nutzungscodeübertragung in Zugangsberechtigungssystemen mit elektronischer Schlüsselcodierung üblich ist und daher hier nicht näher beschrieben zu werden braucht.

Die obige Beschreibung eines bevorzugten Ausführungsbeispiels macht die zuvor erwähnten Vorteile der erfindungsgemäßen Fremdnutzungsschutzeinrichtung deutlich. Es versteht sich, daß sich die Einrichtung sowohl für einen Fuhrpark mit einer begrenzten Anzahl von Fahrzeugen, z.B. eines Speditions-, eines Mietwagen- oder eines Taxiunternehmens, als auch grundsätzlich für alle Fahrzeuge eines betreffenden Gebietes eignet, wobei in letzterem Fall z.B. jeweils nach Zulassung eines Fahrzeugs eine Anforderung zur Abstrahlung der für das Fahrzeug vorgesehenen Nutzungssignale von der Zulassungsstelle zur für die Signalabstrahlung autorisierten Stelle ergehen kann. Das Abstrahlen des jeweiligen Nutzungssignals wird dann von der autorisierten Stelle beendet, wenn sie hierzu von einer berechtigten Person aufgefordert wird, z.B. vom berechtigten Fahrzeugnutzer, dessen Versicherung oder von der Zulassungsstelle nach Abmelden des Fahrzeugs. Außerdem kann die Einrichtung für eine Mietfahrzeugflotte dergestalt verwendet werden, daß die Nutzungssignalabstrahlung von vornherein auf die jeweilige Mietdauer beschränkt wird, wodurch verhindert wird, daß angemietete Fahrzeuge über die Mietdauer hinaus unberechtigterweise weiterbenutzt werden.

Die erfindungsgemäße Einrichtung stellt damit ein sehr zuverlässiges, manipulationssicheres und komfortables System zum Schutz von Fahrzeugen gegen unberechtigte Fremdnutzung dar, wobei nicht das direkte Entwenden verhindert, sondern selbiges dadurch uninteressant gemacht wird, daß das Fahrzeug jederzeit von zentraler Stelle immobilisiert werden kann. Der Aufwand für ggf. zusätzlich vorgesehene Zugangskontrollen, Schließsysteme oder herkömmliche Wegfahrsperren kann damit entfallen oder jedenfalls geringer ausfallen.

Patentansprüche

1. Fremdnutzungsschutzeinrichtung für ein Kraftfahrzeug, mit
 - einer fahrzeugseitig angeordneten Nutzungssteuerungseinrichtung (4), die den Betrieb

wenigstens eines fahrbetriebsnotwendigen Fahrzeugaggregates (5) in Abhängigkeit von einer zugeführten Nutzungsberechtigungsinformation freigibt oder sperrt, wobei

- die Nutzungsberechtigungsinformation von einer oder mehreren fahrzeugexternen Sende-
einheiten (1) mittels einer Übertragungsstrecke
(3) auf Basis elektromagnetischer Wellen abge-
strahlt wird und in vorgegebenen Zeitabständen
periodisch aufeinanderfolgende, fahrzeugspe-
zifische Nutzungssignale beinhaltet und
- die Nutzungssteuerungseinrichtung (4) den
Betrieb des wenigstens einen fahrbetriebsnot-
wendigen Fahrzeugaggregates (5) jeweils nach
Empfang eines Nutzungssignals für eine vorge-
gebene Zeitdauer, die größer als der Zeitab-
stand zweier aufeinanderfolgender
Nutzungssignale ist, freigibt sowie dessen
Betrieb sperrt, wenn sie während der vorgege-
benen Zeitdauer kein weiteres Nutzungssignal
empfängt.

2. Fremdnutzungsschutzeinrichtung nach Anspruch 1,
weiter

dadurch gekennzeichnet, daß

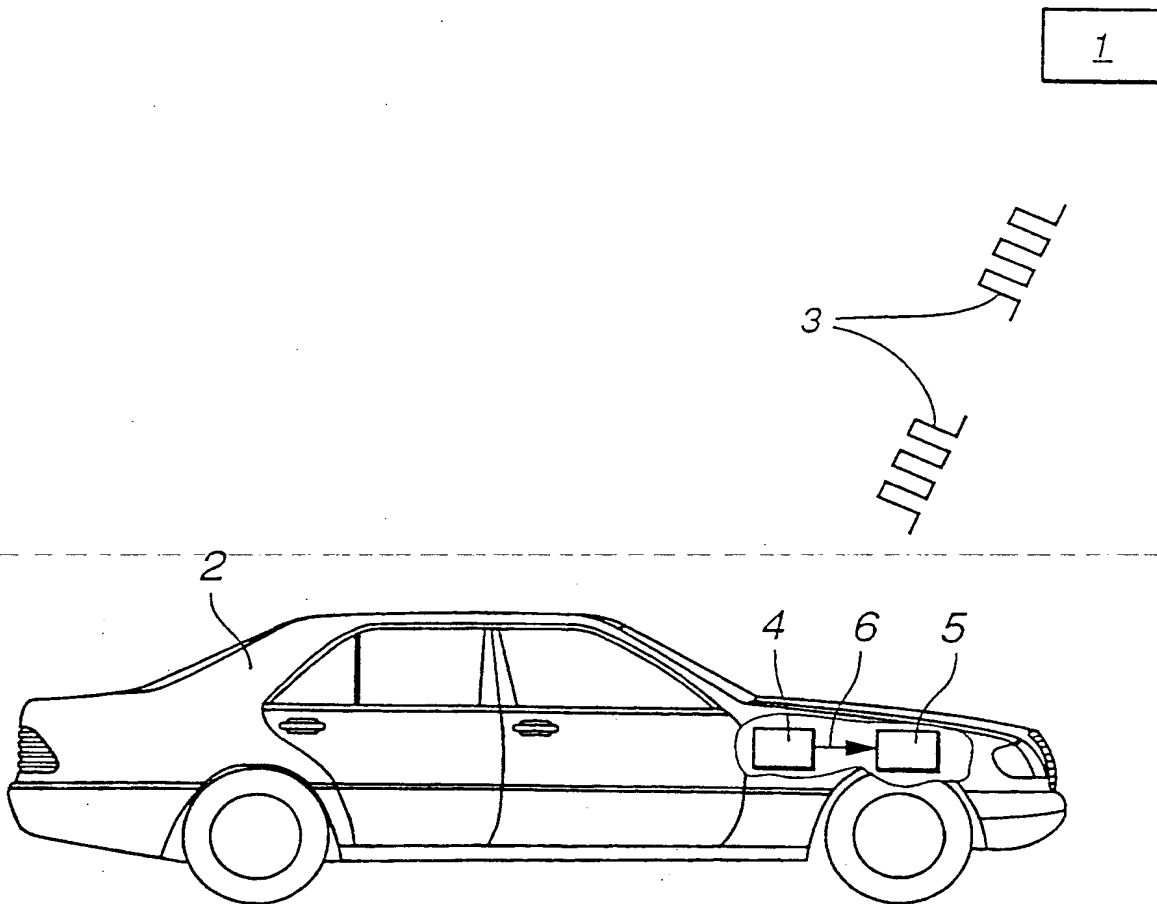
die Nutzungsberechtigungsinformation über ein
digitales Funknetz (3) übertragen wird.

3. Fremdnutzungsschutzeinrichtung nach Anspruch 2,
weiter

dadurch gekennzeichnet, daß

die Nutzungssteuerungseinrichtung (4) ein Autote-
lefon zum Empfang der Nutzungsberechtigungs-
information umfaßt.

This Page Blank (uspto)



①9 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑫ Offenlegungsschrift
⑪ DE 37 17 022 A1

⑳ Aktenzeichen: P 37 17 022.8
㉑ Anmeldetag: 21. 5. 87
㉒ Offenlegungstag: 15. 12. 88

⑤① Int. Cl. 4:
H 04 L 11/26
H 04 H 1/00
H 04 B 1/06
H 04 N 7/00

DE 3717022 A1

⑦① Anmelder:

Deutsche Thomson-Brandt GmbH, 7730
Villingen-Schwenningen, DE

⑦② Erfinder:

Platte, Hans-Joachim, Dr.-Ing., 3005 Hemmingen,
DE; Meier-Engelen, Egon, Dipl.-Ing., 5090
Leverkusen, DE; Plenge, Georg, Prof. Dr., 8195
Egling, DE; Le Floch, Bernard, Dipl.-Ing., Rennes, FR;
Nederlof, Dirk, Dipl.-Ing., Eindhoven, NL; Vollmer,
Rudolph, Dr.-Ing., 3201 Barienrode, DE

⑤⑥ Für die Beurteilung der Patentfähigkeit
in Betracht zu ziehende Druckschriften:

DE	35 20 395 C1
DE	35 09 562 A1
DE	34 40 379 A1
DE	30 36 804 A1
DE	29 26 013 A1
EP	02 03 424 A2

⑤④ Datenübertragungssystem

Die Erfindung betrifft ein Datenübertragungssystem, insbesondere ein digitales Hörfunk- oder Fernseh-Rundfunkübertragungssystem, mit individuelle Adressen aufweisenden Empfangsgeräten. Erfindungsgemäß sind - simultan oder seriell zu Programmbeiträgen (»Nutzdaten«) - Adreßdaten übertragbar, das jeweilige Empfangsgerät enthält eine Prüfschaltung, in der die empfangenen Adreßdaten laufend auf Übereinstimmung mit der individuellen Adresse des Empfangsgerätes überprüft werden (Koinzidenz), und bei Koinzidenz wird das jeweilige Empfangsgerät oder eine ihm zugeordnete Einrichtung automatisch dauerhaft gestört. Unbefugtes Betreiben der Empfangsgeräte, beispielsweise nach einem Diebstahl oder bei Nichtentrichtung von Rundfunkgebühren, wird so weitgehend vermieden.

DE 3717022 A1

Patentansprüche

1. Datenübertragungssystem, insbesondere digitales Hörfunk- oder Fernseh-Rundfunkübertragungssystem, mit individuelle Adressen aufweisenden Empfangsgeräten, **dadurch gekennzeichnet**, daß — simultan oder seriell zu Programmbeiträgen ("Nutzdaten") -Adressdaten übertragbar sind, daß das jeweilige Empfangsgerät eine Prüfschaltung enthält, in der die empfangenen Adressdaten laufend auf Übereinstimmung mit der individuellen Adresse des Empfangsgerätes überprüft werden (Koinzidenz), und daß bei Koinzidenz das jeweilige Empfangsgerät oder eine ihm zugeordnete Einrichtung automatisch dauerhaft gestört wird.
2. Datenübertragungssystem nach Anspruch 1, dadurch gekennzeichnet, daß bei Koinzidenz das jeweilige Empfangsgerät oder eine ihm zugeordnete Einrichtung automatisch dauerhaft außer Funktion gesetzt wird.
3. Datenübertragungssystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Prüfschaltung in einem nicht zerstörungsfrei zerlegbaren Modul (integrierter Schaltkreis) enthalten ist, das dem Empfangsgerät zugeordnete wesentliche Schaltungsteile oder Teile von Steuerschaltungen für wesentliche, dem Empfangsgerät zugeordnete Schaltungsteile enthält.
4. Datenübertragungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß bei Koinzidenz ein in dem Modul enthaltener, den bestimmungsgemäßen Gebrauch des Empfangsgerätes ermöglichender Schaltungsteil dauerhaft in seiner Funktion gestört wird.
5. Datenübertragungssystem nach Anspruch 4, dadurch gekennzeichnet, daß die Funktionsstörung durch irreversibles Schließen oder Öffnen einer in dem Modul enthaltenen Halbleiterstrecke, insbesondere eines p-n- oder n-p-Überganges eines Transistors oder einer Diode bewirkt wird.
6. Datenübertragungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß bei Koinzidenz eine vorbestimmte akustische und/oder optische Ausgabe ("Diebstahl", "Gebühr nicht bezahlt") am Empfangsgerät erfolgt.
7. Datenübertragungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die individuelle Adresse in einem nicht-flüchtigen, im allgemeinen nur einmal, vorzugsweise bei Herstellung oder Verkauf des Empfangsgerätes beschreibbaren Speicher gespeichert ist, und daß der Speicher in dem Modul enthalten ist.
8. Datenübertragungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zwei oder mehr individuelle Adressen je Empfangsgerät vorgesehen sind, denen voneinander unterschiedliche akustische und/oder optische Ausgaben am betreffenden Empfangsgerät zugeordnet sind.
9. Datenübertragungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß ein in ein Fahrzeug eingebautes Empfangsgerät bei Koinzidenz eine dauerhafte Funktionsstörung am Fahrzeug auslöst.
10. Datenübertragungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß ein in ein Fahrzeug eingebautes Empfangsgerät bei Koinzidenz eine deutlich erkennbare Mar-

kierung des Fahrzeuges (z.B. Warnblinker, Hupe, Funksignal) auslöst.

11. Datenübertragungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als individuelle Adresse des Empfangsgerätes ein individuelles Kennzeichen (z.B. Paß- oder Ausweisnummer) des Käufers oder Besitzers des Empfangsgerätes oder des Halters desjenigen Fahrzeuges vorgesehen ist, in das das Empfangsgerät eingebaut ist.

Beschreibung

Die Erfindung betrifft ein Datenübertragungssystem, insbesondere ein digitales Hörfunk- oder Fernseh-Rundfunkübertragungssystem, mit individuelle Adressen aufweisenden Empfangsgeräten. Solche Datenübertragungssysteme, bei denen jeder einzelne Empfänger eine individuelle, nicht oder nur schwer manipulierbare Adresse aufweist und bei denen im Übertragungskanal eine Übertragung von Adressen möglich sind, sind als drahtgebundene oder drahtlose Systeme bekannt, z.B. bei herkömmlichen leitungsgebundenen Fernmeldenetzen, Funktelefonen, oder dergleichen.

Als Folge ständiger Miniaturisierung bei elektronischen Bauteilen ist es gelungen, die bei solchen Datenübertragungssystemen verwendeten Empfangsgeräte in ihren Abmessungen und in ihrem Gewicht erheblich zu reduzieren. So sind mittlerweile auch hochwertige, zum Teil als Tonband/- oder CD/Rundfunk-Kombigeräte ausgebildete Empfangsgeräte problemlos in Kraftfahrzeuge einzubauen. So sehr die Miniaturisierung allgemein wegen der damit verbundenen Mobilität der Geräte zu begrüßen ist, hat sie doch den gravierenden Nachteil, daß diese Geräte in zunehmenden Maße Diebstählen oder Diebstahlsversuchen zum Opfer fallen. Insbesondere sind so im Versicherungswesen in jüngerer Vergangenheit permanent steigende Schadenskosten für Autoradio-Diebstähle, Schäden und Versicherungsbetrügereien zu verzeichnen.

Aus etwas anderen Gründen besteht auch seitens Sendestationen betreibender Rundfunkanstalten der Wunsch, den Betrieb nur solcher Empfangsgeräte zu ermöglichen, für die bestimmte Kriterien erfüllt sind, beispielsweise Gebühren entrichtet werden.

Der Erfindung liegt die Aufgabe zugrunde, ein Datenübertragungssystem zu schaffen, bei dem unbefugtes Betreiben von Empfangsgeräten weitgehend vermieden wird.

Diese Aufgabe wird bei einem Datenübertragungssystem der eingangs genannten Art durch die im Anspruch 1 angegebenen Merkmale gelöst.

Das erfindungsgemäße Datenübertragungssystem hat den Vorteil, daß ein Diebstahl oder ein unbefugtes Betreiben von Empfangsgeräten von vornherein als nutzlos gelten kann. In jüngerer Zeit häufiger in Erscheinung tretende Versuche von Versicherungsbetrügn mit als gestohlen gemeldeten Empfangsgeräten — insbesondere Autoradiogeräten —, die jedoch keineswegs gestohlen worden waren, stellen sich bei dem erfindungsgemäßen Datenübertragungssystem als in gleicher Weise nutzlos dar wie der Diebstahl solcher Geräte selbst. In beiden Fällen läßt sich bei erfindungsgemäßen Empfangsgeräten eine unbefugte Benutzung verhindern.

Bei einem bevorzugten Ausführungsbeispiel der Erfindung wird die Adresse des betreffenden Empfangsgerätes, dessen unbefugtes Benutzen verhindert werden

soll, über eine autorisierte Stelle an einen zentralen Steuerrechner übermittelt. Letzterer übernimmt die Adresse in eine von ihm geführte Liste gestohlener Empfänger bzw. säumiger Rundfunkgebührenzahler. Diese Liste wird — versehen mit entsprechendem Fehlerschutz — in dauernder Wiederholung mit dem eigentlichen digitalen Nutz-Rundfunksignal gemultiplext übertragen. Die Adressen der gemeldeten Empfangsgeräte bleiben entweder für eine begrenzte Zeit (z.B. einige Monate oder Jahre) oder gegebenenfalls bis zum Wiederauffinden des Gerätes bzw. bis zur erfolgten Gebührenzahlung in der — gegebenenfalls jeweiligen — Liste des Zentralrechners.

Als autorisierte Stellen können etwa Polizeidienststellen, Versicherungsagenturen, Inkassostellen für Rundfunkgebühren, oder dergleichen vorgesehen sein.

Ist die dem Empfangsgerät zugeordnete Adresse in Weiterbildung der Erfindung mit einem Personenkennzeichen des Käufers, Besitzers oder Fahrzeughalters, z.B. mit dessen Personalausweis- oder Paßnummer, identisch, so hat dies den Vorteil, daß die Adresse — im Gegensatz zu einer abstrakten laufenden Fertigungsnummer, die der Radiobesitzer häufig nicht zur Hand haben wird — aufgrund der allgemeinen Ausweispflicht stets verfügbar ist.

Bei in Betrieb befindlichem Empfangsgerät werden die übertragenen Adressen laufend auf Koinzidenz einer empfangenen Adresse mit der individuellen Adresse des Empfangsgerätes verglichen. Das Empfangsgerät wird nur solange ungestört arbeiten, wie es nicht seine eigene Adresse empfängt. Wird jedoch die eigene Adresse zweifelsfrei im Adressdatenstrom erkannt, so wird das Empfangsgerät eine vorbestimmte Reaktion auslösen, die vorzugsweise eine irreversible Funktionsstörung des Empfangsgerätes oder im Falle eines Fahrzeug-Empfangsgerätes eine Betriebsstörung des Fahrzeuges zur Folge hat.

Die Funktionsstörung des Empfangsgerätes kann z.B. durch Selbstzerstörung eines integrierten Schaltkreises mit zentraler Funktion bewirkt werden, welcher nicht frei gehandelt wird und somit nicht durch manipulierende Bastler zu ersetzen ist. Als Betriebsstörung eines Fahrzeuges kann etwa eine Anlaßblockierung oder Zündstörung des Motors ausgelöst werden, wobei allerdings Maßnahmen, welche die Verkehrssicherheit des Fahrzeuges nicht beeinträchtigen, der Vorzug zu geben ist. Als weitere Folge kann bei Vorliegen von Koinzidenz auch ein automatisches Markieren des betreffenden Fahrzeuges mittels Warnblinker, Hupe, Display o.dgl. vorgesehen sein.

Die Adressübertragung kann auch benutzt werden zur nachhaltigen Erinnerung säumiger Zahler von Rundfunkgebühren. Hier bleibt die Adresse der entsprechenden Empfangsgeräte ebenfalls im Zentralrechner so lange gespeichert, bis entsprechende Gebührenzahlung erfolgt ist. Solange das betreffende Empfangsgerät nicht betrieben wird, kann die Ausstrahlung der Adresse keine Schäden am Empfangsgerät verursachen. Wird das Empfangsgerät jedoch betrieben, so erscheint eine "fernausgelöste Selbststörung" — wie im Falle eines Diebstahls — als Gegenmaßnahme durchaus gerechtfertigt und wirkungsvoll.

Bei einem für beispielsweise maximal 4 Milliarden Teilnehmer ausgelegten erfindungsgemäßen digitalen Datenübertragungssystem ist für die Adressen eine Länge von ungefähr 32 Bit vorzusehen. Selbst wenn dann die beträchtliche Anzahl von 600 000 als gestohlen gemeldeten Geräten erreicht werden sollte, würde bei

einer "moderaten" Fehlersicherung sowie einer Adressdatenrate von ca. 5 kBit/s die Übertragung der vollständigen Adressenliste innerhalb von jeweils 1,5 Stunden Dauer erfolgen. Da die Liste laufend wiederholt wird, hätte ein Dieb nach Eingang der Diebstahlmeldung beim Zentralrechner längstens 1,5 h lang Freude am ungestörten Betrieb eines per Diebstahl "erworbenen" Gerätes.

- Leerseite -

This Page Blank (uspt.

(Sicherungseinrichtung zum globalen Schutz von Gegenständen mit elektronischen Komponenten)

Beschreibung

Es ist bekannt, daß sich elektrische Baugruppen durch Funksignale fernsteuern lassen. Eine typische Anwendung ist eine elektronische Alarmanlage und/oder Wegfahrsperre eines Kraftfahrzeuges, die der Benutzer mit einem Sender aktiviert oder deaktiviert. Dabei ist es unerheblich, ob der Sender direkt strahlt (z.B. über Infrarotübertragung) oder öffentliche Funkdienste oder Telefonnetze dazwischen geschaltet sind. Wird allerdings solch ein Diebstahlschutz so ausgeführt, daß das zu schützende Objekt durch Abklemmen oder Überbrücken der Schutzeinrichtung wieder aktiviert werden kann, so ist die Absicherung praktisch nutzlos.

Am Beispiel eines Kraftfahrzeuges sollen die typischen Merkmale und Probleme solch einer Sicherung erläutert werden. Prinzipiell läßt sich aber so eine Sicherung für alle Gegenstände mit einer elektronischen Komponente einsetzen. Hierzu können u.a. gehören: Funktelefone („Handies“), (Euro-)Check- und Geldkarten, Kreditkarten, Telefonkarten, Schlüssel für elektronische Schließanlagen, bewegliche elektronische Geräte wie Kassettenrecorder, CD-Spieler, Uhren, Computer usw.

Es ist bekannt, daß Fahrzeuge mit mechanischen und/oder elektrischen Diebstahlschutzvorrichtungen durch Ausbau oder Überbrückung der Sicherung wieder betriebsbereit gemacht werden können. Dies lohnt sich insbesondere bei teuren Fahrzeugen, wo das gesamte Fahrzeug durch organisierte Banden einfach abtransportiert wird und an sicherer Stelle bearbeitet wird. Weiterhin ist bekannt, daß Fahrzeuge mit einer elektronischen Wegfahrsperre, die oft Teil der Motorsteuerung ist, nur unter großem Aufwand und mit Spezialkenntnissen wieder aktiviert werden können. Oftmals ist eine Reaktivierung nur mit einem Originalschlüssel und/oder durch Hinzuziehung einer Vertragswerkstatt möglich.

Da mit einem geraubten Originalschlüssel das Fahrzeug sofort betriebsbereit ist, wird derzeit eine Veränderung vom einfachen Fahrzeugdiebstahl hin zum Diebstahl mit Personenbedrohung beobachtet. Eine Deaktivierung durch einen kleinen Handsender auf einige hundert Meter Entfernung wäre zwar denkbar, birgt aber wieder die Gefahr, daß das Opfer sich selbst in Gefahr begibt, wenn der Täter von der Existenz dieses Senders weiß.

-2-

Um den Schutz der rechtmäßigen Eigentümer wieder sicherzustellen, wurden auch schon Konzepte angedacht, bei dem das Fahrzeug regelmäßig über Funk Signale zur Freischaltung der Elektronik erhält und beim Ausbleiben dieser Signale deaktiviert wird. Bei einem gestohlenen Fahrzeug können dann diese Signale gezielt abgeschaltet werden, so daß das Fahrzeug nicht mehr betriebsbereit ist. Dies hat allerdings den Nachteil, daß bei Auftreten eines Funkloches, wie es auch bei Mobiltelefonen immer wieder der Fall ist, eine Weiterfahrt nicht mehr möglich ist. Zudem muß eine lückenlose Überdeckung des Funkbereiches auch im Ausland gewährleistet sein, da eine temporäre Abschaltung der Sicherung für Auslandsaufenthalte den Schutz wieder ad absurdum führen würde. Eine solche Sicherung bedeutet deshalb starke Einschränkungen für den legalen Besitzer und ist daher am Markt nicht durchsetzbar.

Es ist außerdem bekannt, daß es Vorrichtungen gibt, bei denen durch Funksignale ein Schalter im Fahrzeug aktiviert werden kann, der die Zündungselektronik deaktiviert. Solche Systeme werden durch eine Telefonverbindung realisiert, die der Benutzer durch Anwählen einer bestimmten Nummer, die dem Fahrzeugempfänger zugeordnet ist, aktiviert. Hierbei wäre auch eine globale Erreichbarkeit des Fahrzeuges denkbar. Diese Systeme können jedoch dadurch umgangen werden, daß der Empfänger aus dem Fahrzeug ausgebaut wird oder durch eine entsprechende Abschirmung am Empfang der Signale gehindert wird, so daß eine Blockierung der Zündelektronik nicht mehr erfolgt.

Für eine universelle Sicherung muß daher das System so gebaut sein, daß eine Reaktivierung nicht durch den Benutzer selbst erfolgen kann, denn sonst könnte man ja durch Erpressung die hierzu nötigen Informationen erhalten. Weiterhin muß die Deaktivierung des Systems auch nach dem Diebstahl zu einem beliebigen Zeitpunkt erfolgen können. Diese Deaktivierung kann auch durch Dritte erfolgen, so daß sich eine Bedrohung oder gar Tötung des Eigentümers nicht auszahlt. Für einen Dieb wird daher der Diebstahl eines solchen Objektes wertlos, da es innerhalb weniger Stunden seine gewünschte Funktionalität nicht mehr haben wird.

Funktionsweise

Die Erfindung vermeidet die oben genannten Nachteile, indem zumindest eine der Baugruppen 5,6,7,8 (Figur 1) und/oder Informationen innerhalb zumindest einer dieser Baugruppen, die für den Betrieb des Fahrzeugs essentiell sind, irreversibel deaktiviert und/oder gelöscht werden, so daß auch ein Ausbau oder eine Überbrückung der betreffenden Komponenten keine Wirkung

-3-

erzielt, da die Beschaffung eines funktionsfähigen Ersatzteils unumgänglich ist. Diese Baugruppen können z.B. in der Motorelektronik 6, dem Lenkradschloß 7, dem Türschloß 8 und/oder dem Schlüssel 5 untergebracht sein.

Zur Erzielung eines weltumspannenden Schutzes wird das Funksignal 9,14 vorzugsweise von einem niedrig fliegenden Satelliten und/oder einer Raumstation 1, beide mit hoher Inklination - um eine globale Bedeckung zu erreichen - ausgestrahlt. Dabei ist es nicht nötig, in einer polaren Bahn mit 90° Inklination zu fliegen, da der Sender 2 eine gewisse Seitenreichweite 19 hat und schon bei etwa 50° Inklination durch die Drehung der Erde der Bereich der bewohnten Erdoberfläche 16 abgedeckt wird (Figur 2). In den nicht abgedeckten Bereichen 17,18 an den Polen ist diese Anwendung uninteressant, da es hier keine Konsumenten gibt. Bei den heute üblichen Funkdichten und Beschränkungen der Sendeleistungen kommt zur Zeit hierfür vorzugsweise eine Raumstation 1 in Betracht, da sie über einen längeren Zeitraum in den für die Erzeugung der erforderlichen Empfangsfeldstärke maximalen Flughöhen bis 400 km gehalten werden kann. Die Ansteuerung des Senders 2 kann über Funk oder andere Kommunikationsmittel erfolgen, z.B. durch Anruf bei einer Notzentrale 3, die die entsprechende Aktivierung 20 des Senders 2 übernimmt.

Bei einem Diebstahl des Fahrzeuges 4 mit Schlüssel 5 oder einer erpresserischen Übernahme des Schlüssels 5 ruft der legitime Fahrzeugeigentümer telefonisch eine Servicenummer an oder er übermittelt durch andere Art und Weise die Anzeige des Diebstahls. Nach einer Überprüfung seiner Authentizität, z.B. durch Angabe eines Paßwortes um böswillige Deaktivierungen zu verhindern, wird durch eine oder mehrere Bodenstationen 3 die Identifikationsnummer der gestohlenen Einheit an den Sender 2 im Orbit übermittelt. Diese Identifikationsnummer (ID) ist vorzugsweise weltweit eindeutig für jeden Empfänger und/oder Empfängergruppe 5,6,7,8 vergeben und kann z.B. in einer Datenbank abgelegt sein. Der Sender 2 im Weltall sendet nun vorzugsweise periodisch diese ID aus, so daß im Verlauf der Zeit auf der gesamten Erdoberfläche 16 das Signal 9,14 empfangen werden kann.

Die Diebstahlsicherung 6,7,8 im Fahrzeug löscht bei Erkennen des für sie bestimmten Signals 9 irreparabel wichtige Informationen und/oder zerstört Bauelemente vorzugsweise innerhalb der Bordelektronik, des Schlüssels und/oder des Schlosses, ohne die eine Funktion des Fahrzeuges 4 nicht möglich ist. Der Empfänger bzw. die Dekodierlogik 9 und die sicherheitsrelevanten Baugruppen 10 bilden vorzugsweise eine Einheit 21 (z.B. Mikroprozessor mit eigenem,

-4-

internen Speicher), damit nicht der Datenverkehr 11 der Elektronik „belauscht“ und möglicherweise so manipuliert werden kann, daß keine Deaktivierung mehr erfolgen kann.

Zusätzlich zur Deaktivierung kann das Fahrzeug 4 auch Signale zurücksenden, die eine leichtere Lokalisierung ermöglichen, für den Schutz des Fahrzeuges ist dies jedoch nicht unbedingt erforderlich. Das System kann außerdem so gebaut sein, daß nur der legitime Besitzer dieses Signal auslösen kann, damit nicht eine unerwünschte permanente Ortung des Fahrzeuges möglich wird.

Die deaktivierten Baugruppen können durch Überprüfen der Seriennummer und/oder der zerstörten Daten auch nachträglich noch als gestohlen identifiziert werden. Hierzu kann z.B. eine Vertragswerkstatt ein entsprechendes Diagnosegerät verwenden, mit dem die Daten der Baugruppen 5,6,7,8 ausgelesen werden. Um Fehlalarme und mutwillige Deaktivierungen auszuschließen, kann das Signal 9,14 mit Prüfsummen versehen werden, die einen Übertragungs- und/oder Authentizitätsfehler erkennen lassen.

Aus Sicherheitsgründen wird man vorzugsweise bei einem Fahrzeug, das gerade fährt, ein geregeltes, langsames Abschalten vornehmen, so daß die Gefahr eines Unfalles vermieden wird. Dies kann z.B. so geschehen, daß das Fahrzeug nicht mehr beschleunigt werden kann und allmählich immer langsamer wird bis ein Stillstand erreicht wird. Anschließend kann der Motor abschaltet werden. Dabei ist es irrelevant, ob die Deaktivierung sofort erfolgt oder erst einige Zeit, nachdem das Diebstahlsignal abgesetzt wurde. Für den potentiellen Dieb wird die Entwendung eines solchen Fahrzeugs uninteressant, da das Fahrzeug nach der Entwendung jederzeit stehen bleiben kann und unbenutzbar wird.

Es ist auch möglich, diesen Empfänger nicht nur im Fahrzeug 4 selbst, sondern auch im Schlüssel 5 unterzubringen (Verteilte Sicherheit). Moderne Wegfahrsperren verwenden vorzugsweise keine mechanischen Schlösser mehr, sondern tauschen zwischen Schlüssel und Fahrzeug verschlüsselte Codes 12 aus, die das Fahrzeug entsperren. Im Falle einer Deaktivierung durch ein Funksignal 9,14 reicht es daher aus, wenn zumindest eine der Komponenten 5,6,7,8 den Abschaltcode erhalten hat. Beim nächsten Versuch, das Fahrzeug 4 zu starten, breitet sich die Information durch den Datenaustausch 15 vorzugsweise auf alle Komponenten aus, die sich nun ihrerseits wie oben beschrieben deaktivieren. Dieser Datenaustausch kann ebenfalls nicht unterbunden werden, z.B. durch das Einspielen von synthetischen Informationen, da die Signalisierung durch das Ausbleiben der richtigen Daten

12 erfolgt. Diese Daten 12 werden bei jeder Kontaktaufnahme der Komponenten 5,6,7,8 neu generiert und können nur von diesen erzeugt und entschlüsselt werden, da die Komponenten bei der Herstellung aufeinander abgeglichen werden (Prinzip der Einmal-Codes).

Eine „Reparatur“ des Fahrzeuges ist also anschließend nur durch Tausch vorzugsweise aller deaktivierten Komponenten 5,6,7,8 gleichzeitig möglich. Eine Vertragswerkstatt kann beim Verkauf der neuen Baugruppen, die natürlich nur unter Rückgabe mindestens einer der deaktivierten Komponenten 5,6,7,8 erfolgt, feststellen, ob ein Diebstahlsignal 9,14 für die Deaktivierung verantwortlich war und so den Dieb beim Versuch, das Fahrzeug 4 umzubauen und wieder zu reaktivieren, dingfest machen. Der Vorwand, die Komponenten seien bei einem Unfall zerstört worden und könnten daher nicht vorgelegt werden, hilft hier auch nicht weiter, da ein Unfall, bei dem sämtliche Elektronikmodule 6,7,8 sowie alle Schlüssel 5 zerstört wurden, nicht vorkommen kann. Auch die Abgabe eines unversehrten Schlüssels 5, der kein Deaktivierungssignal 14 empfangen hatte, ist nutzlos, da in diesem Fall das Auslesen der ID und ein Abgleich mit der Datenbank sofort einen Diebstahl aufzeigt.

Die verteilte Sicherheit erhöht außerdem die Zuverlässigkeit des Systems, da Fahrzeuge unter Umständen in Bereichen abgestellt werden, wo ein Empfang der Funksignale 9,14 nicht ständig möglich ist (Tiefgarage o.ä.) oder der Empfänger absichtlich abgeschirmt wird. Es darf für den legalen Benutzer aber nicht der Fall eintreten, daß das Gerät durch schlechte Empfangsbedingungen fälschlicherweise deaktiviert wird. Ein im Schlüsselanhänger integrierter Empfänger 13 wird normalerweise hinreichend oft gute Empfangsbedingungen haben und kann regelmäßig kontrollieren, ob der Diebstahlfunkdienst 14 fehlerfrei empfangen werden kann. Ist dies nicht der Fall, so geht der jeweilige Empfänger in einen metastabilen Zustand über. Beim nächsten Versuch, das Fahrzeug zu starten, prüfen die Komponenten durch den Abgleich 15 ihrer Daten untereinander, ob mindestens eine der Komponenten innerhalb der zulässigen Zeitspanne ein Signal 9,14 empfangen konnte. Wenn ja, so wird die Anlage vollständig reaktiviert. Wenn nein, so wird dem Benutzer signalisiert, daß innerhalb einer bestimmten Zeitspanne ein Funkkontakt ermöglicht werden muß, da sich ansonsten die Elektronik deaktivieren wird. Läßt der Dieb bei einem gestohlenen Fahrzeug diesen Funkkontakt zu, so wird die Elektronik ebenfalls deaktiviert, so daß in keinem Fall das Fahrzeug 4 für einen Dieb benutzbar bleibt.

Da der Empfänger sehr stark miniaturisiert werden kann, eignet sich dieses System der Deaktivierung auch sehr gut für Geräte, die sowieso Funkkontakte herstellen müssen, wie z.B.

-6-

Funktelefone 21 (Figur 3). Der Empfänger kann dabei in der Chipkarte 22 und/oder dem Telefon 21 untergebracht sein. Wenn eines der Geräte ein Deaktivierungssignal 23,24 empfängt, wird bei der nächsten Inbetriebnahme, bei der die Karte 22 in das Telefon 21 gesteckt werden muß, durch den Datenaustausch 26 der Komponenten untereinander das Telefon 21 und/oder der Chipkarte 22 deaktiviert, wobei das Telefon auch nach einer Deaktivierung weiterhin solche Signale 25 aussenden kann, daß eine Lokalisierung möglich wird.

Prinzipiell läßt sich der Empfänger auch in die neueste Generation von Checkkarten 27 einbauen, so daß hier ein Schutz von EC-, Kredit- und Telefonkarten möglich wird. Eine Karte, die ein Deaktivierungssignal 28, 29 empfängt (dies kann auch aus dem Automaten 30 selbst stammen), kann ebenfalls ihren internen Speicher löschen. Beim nächsten Versuch, die Karte zu benutzen, kann ein Geldautomat 30 dies feststellen und entsprechende weitergehende Maßnahmen einleiten: z.B. Aufzeichnung der Person auf Video, Meldung des Standortes zur Bewegungsbilderstellung, Sperrung der Türen usw.

(Sicherungseinrichtung zum globalen Schutz von Gegenständen mit elektronischen Komponenten)

Patentansprüche

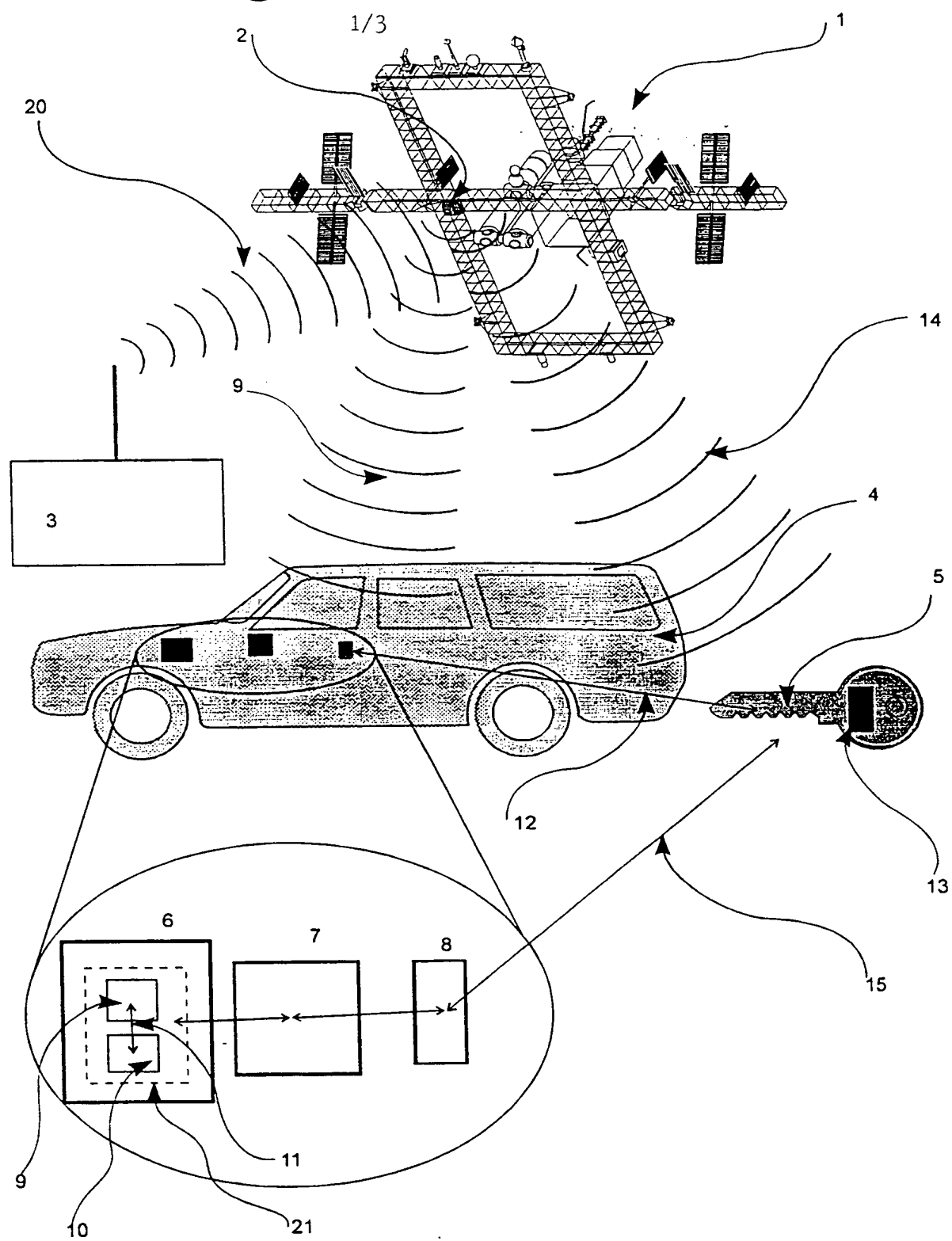
1. Verfahren zum globalen Schutz von Gegenständen mit elektronischen Komponenten, dadurch gekennzeichnet, daß durch ein Funksignal eine oder mehrere Baugruppen und/oder Informationen innerhalb dieser Baugruppen so irreversibel verändert werden, daß eine ganze oder teilweise Weiterbenutzung der Gegenstände mit oder ohne diesen Baugruppen nicht mehr möglich ist.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Funksignale insbesondere von einem oder mehreren Flugkörpern wie Satelliten oder Luftschiffen abgestrahlt werden.
3. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die Aufarbeitung der zu sendenden Signale durch eine Notzentrale oder eine andere zentrale Stelle erfolgt.
4. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß sowohl die Aussendung der Signale als auch die Deaktivierung sofort oder zeitverzögert geschehen.
5. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die Empfänger der Funksignale zusätzlich weltweit eindeutige Kennnummern besitzen.
6. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß diese Kennnummern einmalig oder periodisch ausgesendet werden.
7. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die Empfänger nach dem Erhalt von einer oder mehreren Kennnummern auch Signale vorzugsweise zum Sender zurückschicken können.
8. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die zurückgesendeten Signale außerdem zur Ortung verwendet werden.
9. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die Signale Prüfsummen enthalten, die Übertragungsfehler und/oder Fälschungen erkennen lassen.

10. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß auch das Ausbleiben eines Signals zu einer Deaktivierung der Komponente, der Baugruppe und/oder des Gegenstandes führen kann.
11. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß übermittelten Signale auch an andere Vorrichtungen weitergegeben werden und/oder dort geprüft werden.
12. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die authentische Übermittlung der Signale durch Einmal-Codes gesichert ist.
13. Verfahren nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die Kennnummern in einer Datenbank abgelegt sind.
14. Vorrichtung zum globalen Schutz von Gegenständen mit elektronischen Komponenten, dadurch gekennzeichnet, daß durch ein Funksignal die Vorrichtung Bauelemente und/oder Informationen so verändert, daß der normale Betrieb der Gegenstände nicht mehr möglich ist.
15. Vorrichtung nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die relevanten Bauteile eine Einheit bilden und/oder durch abhörsichere Leitungen verbunden sind.
16. Vorrichtung nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß die erfolgte Deaktivierung und/oder die Identität der Baugruppe auch nachträglich noch überprüft werden kann.
17. Vorrichtung nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß es mehrere getrennte Baugruppen gibt, die jede für sich das Signal auswerten können.
18. Vorrichtung nach Anspruch 17, dadurch gekennzeichnet, daß die Sicherheit auf mehrere Komponenten verteilt ist.
19. Vorrichtung nach Anspruch 17, dadurch gekennzeichnet, daß die Baugruppen den Erhalt und/oder das Ausbleiben des Signals untereinander bestätigen können.
20. Vorrichtung nach Anspruch 17, dadurch gekennzeichnet, daß durch den Austausch von Daten der Komponenten untereinander ebenfalls eine Deaktivierung erfolgen kann.

-9-

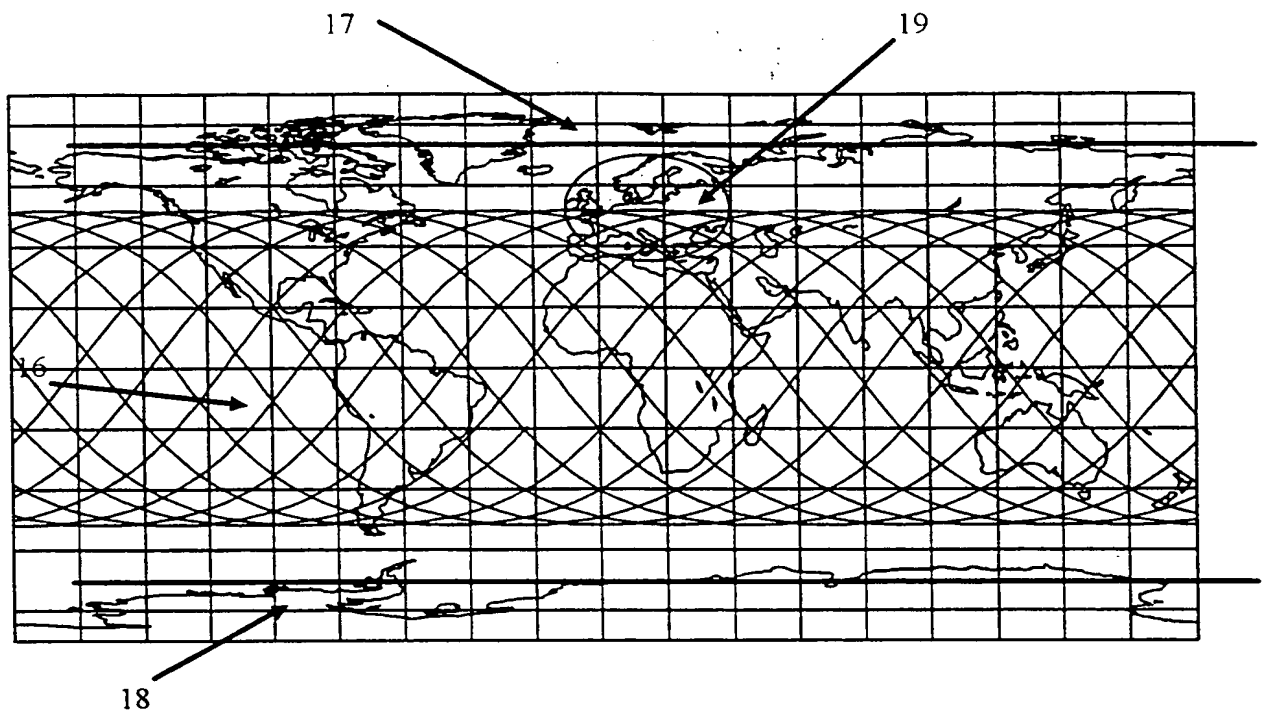
21. Vorrichtung nach Anspruch 20, dadurch gekennzeichnet, daß diese Deaktivierung auch nachträglich erfolgen kann.
22. Vorrichtung nach einem der oberen Ansprüche, dadurch gekennzeichnet, daß eine Reaktivierung nur durch den Tausch von vorzugsweise allen Komponenten erfolgen kann.

This Page Blank (uspto)



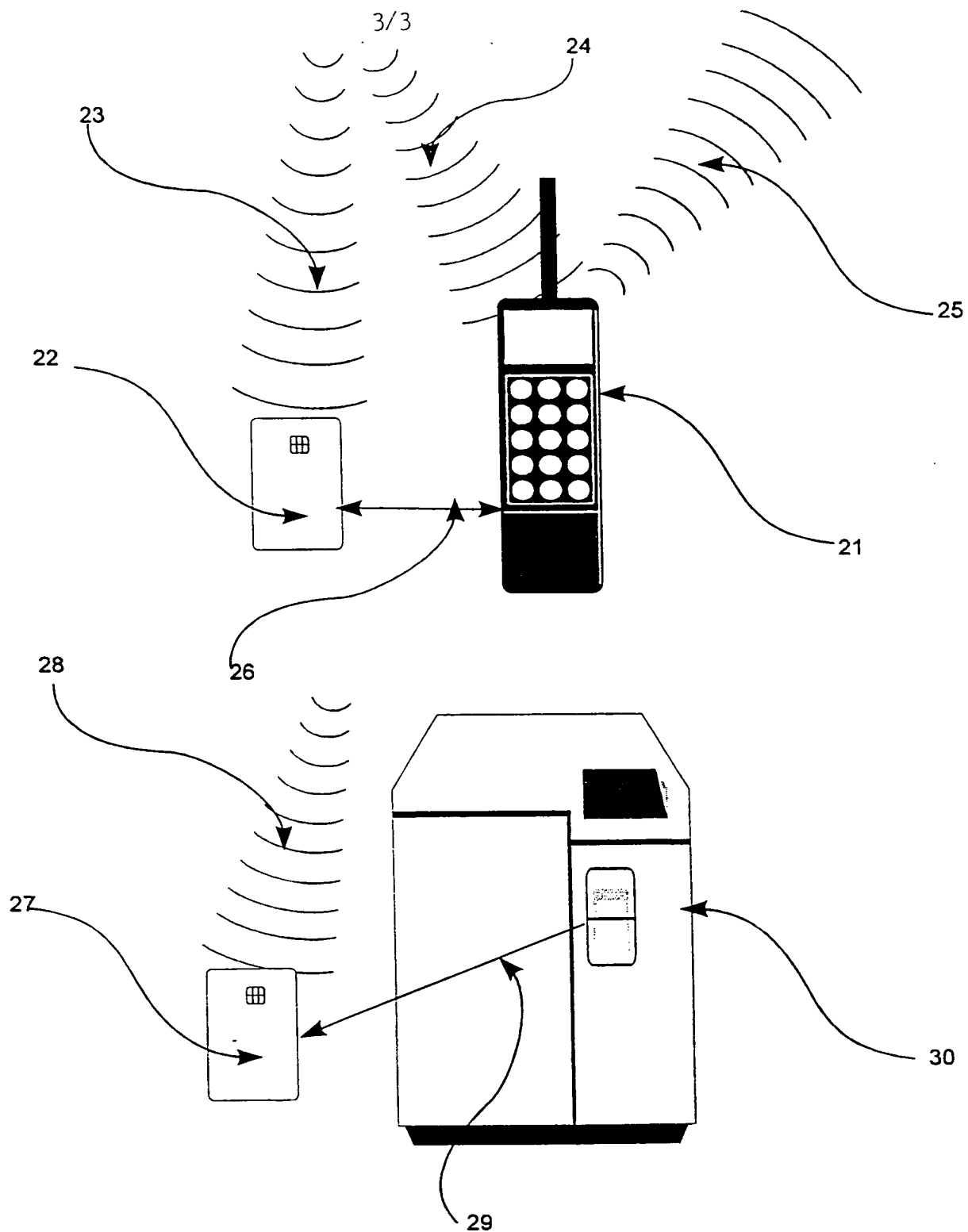
Figur 1

This Page Blank (uspto)



Figur 2

This Page Blank (uspto)



Figur 3

Inis Page Blank (uspro)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/01082

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 B60R25/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 43 18 596 A (KIZLER PETER DR) 8 December 1994	1,3-8, 11,13-22
Y	see abstract; claims; figure see column 1, line 55 - column 6, line 13 ---	2,9,10, 12
Y	US 5 490 200 A (SNYDER BERNARD M ET AL) 6 February 1996	2
A	see abstract; claims 1-3,22; figures 1,2 see column 3, line 12 - column 4, line 50 ---	1,3,4,7, 8,11,14
Y	GB 2 254 461 A (ALPS ELECTRIC CO LTD) 7 October 1992	9,12
A	see abstract; claims 1,2; figures 1-7 see page 7, line 20 - page 13, line 15 ---	1,14
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

7 June 1999

Date of mailing of the international search report

16/06/1999

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Westland, P

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/01082

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 712 768 A (DAIMLER BENZ AG) 22 May 1996	10
A	see abstract; claims; figure see column 2, line 42 - column 4, line 10 ---	1-4, 11, 14, 15
X	DE 37 17 022 A (THOMSON BRANDT GMBH) 15 December 1988 see abstract; claims 1, 2, 4, 8-10 see column 2, line 53 - column 3, line 50 ---	1, 3-6, 11, 14-17, 22
A	GB 2 271 008 A (TELEFUNKEN MICROELECTRON ;DAIMLER BENZ AG (DE)) 30 March 1994 see abstract; claims 1-5; figures see page 2, line 5 - page 4, line 17 -----	1, 11, 14-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/01082

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
DE 4318596	A	08-12-1994	NONE	
US 5490200	A	06-02-1996	AU 8072894 A CA 2130507 A WO 9513943 A US 5588038 A	06-06-1995 20-05-1995 26-05-1995 24-12-1996
GB 2254461	A	07-10-1992	JP 4306380 A JP 2807100 B DE 4204463 A	29-10-1992 30-09-1998 27-08-1992
EP 0712768	A	22-05-1996	DE 4440975 A US 5711392 A	23-05-1996 27-01-1998
DE 3717022	A	15-12-1988	WO 8809588 A EP 0291995 A PT 87521 A	01-12-1988 23-11-1988 31-05-1989
GB 2271008	A	30-03-1994	DE 4232435 C FR 2696137 A US 5583479 A	25-11-1993 01-04-1994 10-12-1996

This Page Blank (uspto)

2

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	GB 2 254 461 A (ALPS ELECTRIC CO LTD) 7. Oktober 1992	9,12
A	siehe Zusammenfassung; Ansprüche 1,2; Abbildungen 1-7 siehe Seite 7, Zeile 20 - Seite 13, Zeile 15	1,14
Y	EP 0 712 768 A (DAIMLER BENZ AG) 22. Mai 1996	10
A	siehe Zusammenfassung; Ansprüche; Abbildung siehe Spalte 2, Zeile 42 - Spalte 4, Zeile 10	1-4,11, 14,15
X	DE 37 17 022 A (THOMSON BRANDT GMBH) 15. Dezember 1988	1,3-6, 11, 14-17,22
	siehe Zusammenfassung; Ansprüche 1,2,4,8-10 siehe Spalte 2, Zeile 53 - Spalte 3, Zeile 50	
A	GB 2 271 008 A (TELEFUNKEN MICROELECTRON ;DAIMLER BENZ AG (DE)) 30. März 1994 siehe Zusammenfassung; Ansprüche 1-5; Abbildungen siehe Seite 2, Zeile 5 - Seite 4, Zeile 17	1,11, 14-20

INTERNATIONALER RESEARCHENBERICHT

Angaben zu Veröffentlichung, d. h. die derselben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/01082

Im Recherchenbericht angeführtes Patendokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4318596 A	08-12-1994	KEINE	
US 5490200 A	06-02-1996	AU 8072894 A CA 2130507 A WO 9513943 A US 5588038 A	06-06-1995 20-05-1995 26-05-1995 24-12-1996
GB 2254461 A	07-10-1992	JP 4306380 A JP 2807100 B DE 4204463 A	29-10-1992 30-09-1998 27-08-1992
EP 0712768 A	22-05-1996	DE 4440975 A US 5711392 A	23-05-1996 27-01-1998
DE 3717022 A	15-12-1988	WO 8809588 A EP 0291995 A PT 87521 A	01-12-1988 23-11-1988 31-05-1989
GB 2271008 A	30-03-1994	DE 4232435 C FR 2696137 A US 5583479 A	25-11-1993 01-04-1994 10-12-1996

This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)